Malware Inc. - Firefox

Malware Inc. is a project that aims to study the development of Malware on various platforms, such as Web browsers, Social networks and Web engines. I chose Mozilla Firefox as my research platform, as it is the second most widely used web browser today. Having a wide audience adds to the importance of this research project, because the security of a higher number of people is at stake. My role in this research project was to study Firefox extensions, small pieces of code that help in enhancing the browsing experience. These extensions, although very helpful, have the potential to be used for malicious purposes.

At the time of the beginning of the Project, Firefox 4 was the latest version of the browser available. This browser was significantly different than the older versions of Firefox, and handled extensions in a very different way. I chose to focus on the new version, even though the documentation process was not complete. The old versions would soon be phased out, and it wouldn't be very useful to conduct the research that would be obsolete in a few months time.

The project was officially divided into three phases. The first phase, which was about 2 weeks long, provided a time period to get acquainted with the development environment. A simple extension was expected at the end of phase 1. I was able to successfully develop two major extensions:

1. **LivEdit:** This extension added a few options to an existing Firefox installation, and enabled the user to edit text in a webpage, like deleting text, highlighting important sentences, defining words, and also translating text in place, so the rest of the page is not changed whats over.
2. **Tab Merger:** This was a very basic extension, which basically merges tabs from two or more windows, all into one window, thus reducing the clutter on the user's desktop.

A report on the development process marked the end of phase 1. The aim of these extensions was also to create a legit application that would help us, creators of malicious code, to hide the malicious operations in these legit applications.

The aim of phase 2 was to study the API, and find what is accessible to a developer, and how easy it is to access the data(i.e. Whether it requires special permission or passwords to work). It also required us to write simple code that would demonstrate the above findings. At about 2 weeks into the process of research, we were requested to present to the Pittsburgh Web development class about what we learned in phase 1. This presentation went very well, and was kept simple and to the point.

After about 2 more weeks, Phase 2 was finally over. Mozilla, although having a very good base for information, lacked a lot of details. Several Low-level API's(Which provide access to the most powerful features of the browser) were scarcely documented. I had to finally settle with documentation for older versions of Firefox, which would sometimes not work with Firefox 4. This can be thought of as “Security through obscurity”, which basically means that it is harder to perform powerful commands, just because enough instructions are not available. In today's world, this just doesn't work, as a person with enough persistence can eventually figure out the exact commands available.

Phase 3 was all about implementing and bringing all the findings in phase 2 together. We were required to create actual malware, especially emphasizing on data theft. The purpose of developing malicious code was to help us better understand the internal architecture and structure of Firefox, how the browser handles extensions, how extensions are distributed, how deep is the screening for malicious code on the Firefox website, and how users suspect extensions to be malicious. Understanding all this would also help us be better prepared for securing the browser, although this is a completely separate task altogether.

Phase 3 was around 3-4 weeks long. I managed to successfully code several extensions that were malicious:

1. **Password Stealer:** Firefox uses a password manager to store passwords. This particular extension secretly steals all the user names and passwords stored in the password manager.
2. **Locater:** This extension frequently steals and send the user's current location. Location tracking has been a serious issue, even with the big names such as Apple. Although the Firefox API instructs the developer to provide a dialog that asks the user's permission, it is not forced.
3. **Executor:** This extension basically creates a backdoor into the user's computer, allowing the developer to execute several commands without the user's knowledge. Thus, the developer can access the user's file system, start or stop programs, shutdown the computer, to name a few.
4. **Keylogger:** This extension secretly downloads and execute an external key logging application. This application basically captures all the key strokes and saves them to a file buffer. The extension periodically reads this buffer and sends the contents to the developer. This was actually a proof of concept for the 'capture and send' methodology, and the same kind of implementation can be used to capture the screen, and therefore provide the malicious developer with a constant video stream of the user's desktop.

Looking at previous malware was also part of this phase. Several malware were found, few of which were:

1. **The Ant Video Downloader:** With over seven million downloads, this extension had a 4 out of 5 star rating on the Mozilla website. This malicious software sent back to its servers user data, involving each and every website they visit, even in private browsing mode. Although sending such data is not illegal, the user should be notified, which was not the case with this extension.
2. **FirestarterFox:** Although not very famous, this addon hijacked requests from popular search engines and redirected them through a Russian website, with the intention of displaying ads on the resultant web page.
3. **Sothink Web Video Downloader 4.0:** This extension was downloaded about 4000 times, and contained a full-fledged Trojan Horse designed to hijack Windows machines.
4. **Master Filer:** This extension was not very popular, but it had a similar Trojan Horse targeting Windows machines.

All these findings will be a good starting point for anyone working in the browser security sector, and we aim to be as much of help as we can to this community.